

NETWORK AND COMPUTER SECURITY

SUMMARY

Lorenzo De Bie

Academic year: 2020-2021



CONTENTS

1	Introduction	2
1.1	Security in the media	2
1.2	Example Incidents	3
1.3	Why do we need security? Why Information Security?	3
2	Basic Concepts	4
2.1	A security model	4
2.2	Security Goals	4
2.2.1	Confidentiality	4
2.2.2	Authentication	5
2.2.3	Access Control/authorization	5
2.2.4	Data integrity	6
2.2.5	Non-repudiation	6
2.2.6	Availability	6
2.3	Security Threats	6

1 INTRODUCTION

1.1 Security in the media

- Security \Leftrightarrow User friendly: work of security personnel goes unnoticed when everything is good, but they get blamed when things go wrong.
- Users remains a security risk:
 - Due to lack of knowledge: *1 in 10 in a survey think HTML is an STD - Los Angeles Times* [1]
 - Due to incompetence
 - Information can still be shared non-digitally
- Nobody is safe: *NSA hackt Belgische cyberprof - De Standaard* [2]
- Privacy vs Security: sacrificing privacy so data can be used for security.
 - *AIVD hackt internetfora, 'tegen wet in' - NRC* [3]
 - *Révélation sur le Big Brother français* [4]
- Check yourself using <https://haveibeenpwned.com/>
- Privacy vs Health: tracing apps in times of COVID-19
- Journalists aren't always exactly IT experts \rightarrow remain a critic, remain sceptic
- Future trends: blockchains
 - mainly used for data integrity through **public ledgers**
 - Used to log activity.
 - * Detect malicious operations, hackers, foreign surveillance, database modifications
 - * Equally important as access restrictions
- Future trends: cyber warfare
 - Nation wide actions to cause damage or disruption. Can include physical impact and/or harm to human persons
 - Interesting targets: traffic lights, electricity systems, water filtration, power plants
 - Stuxnet:
 - * Worm that targeted Iranian nuclear facilities, damaging centrifuges and other hardware
 - * Most likely an American-Israeli cyberweapon
 - Petya: ransomware or state attack?
 - * Focused strongly on Ukraine systems
 - * Made very little money
 - * Either very buggy, or very damaging by purpose: permanent removal of files, nuclear power plants, ministries, metros and banks offline, possible link with assassination of Maksym Shapoval
 - Future trends: IoT: *Docs shielded Cheney defibrillator from hacks - CNN* [5]

1.2 Example Incidents

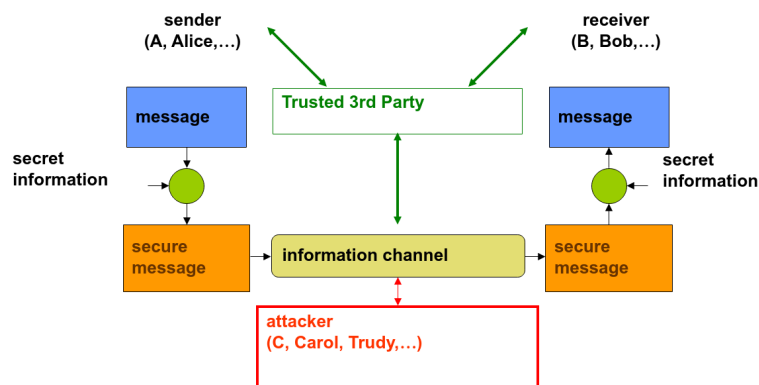
- Ashley Madison (2015)
- DNC email leak (2016)
- Mirai (2016)
- Twitter hack (2020)

1.3 Why do we need security? Why Information Security?

- Counterpart of securing material objects
 - Material object have some **value**
 - Can be stolen or damaged
 - Cost for security/protection takes into account value and risk of theft/damage
- Risk of threats against information security is **much** greater
- Value of information sometimes hard to assess, best estimated by damage caused. Losses cannot be undone
- Threats against information include:
 - **Loss** of information
 - **Forged** information
 - **Unauthorised release** of information
 - **Repudiation** of information
- Value of information systems hard to asses. Systems used to enable service →damage when service unavailable or unreliable
- Threats against information systems include:
 - **Unavailability**/disruption of service
 - **Unauthorised acces** to service
 - Threats against exchanged information
- Security measures for information systems:
 - **Information Security**: encryption, virus scanners, firewalls...
 - Carry some cost (installation, maintenance, computation time)
 - dependent on risk and potential damage

2 BASIC CONCEPTS

2.1 A security model

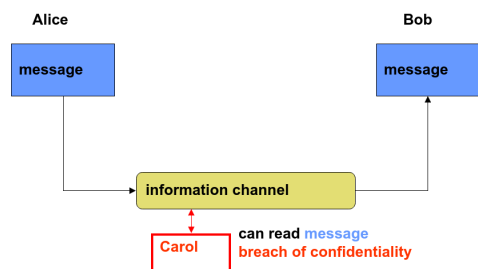


2.2 Security Goals

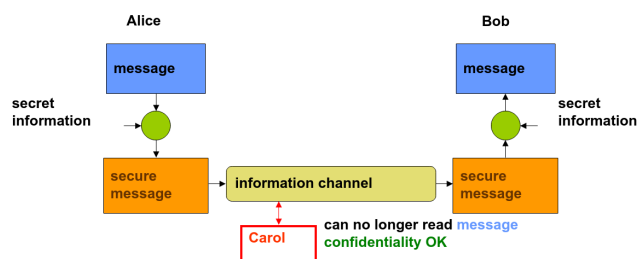
Possible exam question: Which security goals does this protocol fulfill?

2.2.1 Confidentiality

- Data can only be read by those who are allowed to read the data
- Applications:
 - Communicating confidential data between branches of a corporation
 - Passwords
 - Storage of health data



(a) Passive attack by Carol: **eavesdropping** upon information channel



(b) Solution to eavesdropping

Traffic-flow confidentiality

- Keeping secret who's communicating with whom
- Much harder to achieve than data confidentiality

- In Figure 2.1b data confidentiality is OK, traffic-flow confidentiality is NOT OK: Carol can still see that Alice is communicating with Bob

Confidentiality vs Privacy

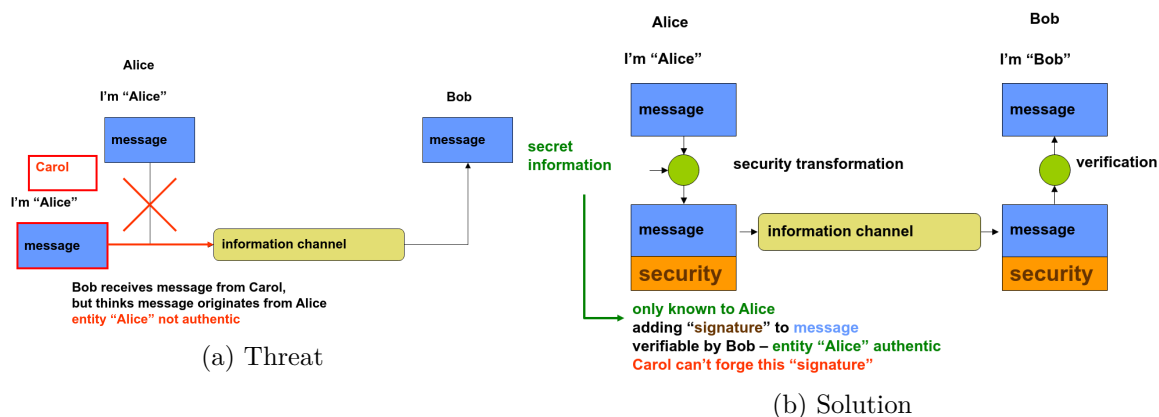
Privacy is having the right to choose what information you give away. It is a fundamental right, legally protected since long. Not every confidentiality requirement involves privacy: intellectual property in a business requires confidentiality, no privacy.

2.2.2 Authentication

Authentication is related to **identification**: it is the *electronic world* equivalent. *Is the person at the other end of the communication who he claims he is?*

Guaranteeing the authenticity of a communication is based on:

- **Entity** authentication: distinguish each entity from another based on collection of data. Each entity has a unique identity.
- **Attribute** authentication. Attribute = characteristic of an entity. Entities are often authenticated through authentication of some of its attributes. Do the communicating parties exhibit the characteristics they claim to have?
- **Data-origin** authentication: does the data indeed originate from the specified source? Important to evaluate whether data is reliable (**Data Integrity** see 2.2.4). Different from entity authentication: **no interaction with data source**.



2.2.3 Access Control/authorization

- Determines which user may access which resource (data, computation time, etc.)
- Requires **authentication of the entity** requesting access to these resources
 - System determines to what extent entity may access those resources
 - Access rights may **depend on entity itself or its attributes**

Illustration 1: access control in OS

- Authentication through login and password
- Access control determined for this user (entity)
 - Full access to own files
 - Limited access to some other files

- No access to other files
- Access rights different from user to user

Illustration 2: access control to medical database

- Different rights for different types of Users
- Requires authentication based on specific **attributes**
- Access rights depend on attributes of the user
- Access rights different from user type to user type (**roles**)

2.2.4 Data integrity

2.2.5 Non-repudiation

2.2.6 Availability

2.3 Security Threats

BIBLIOGRAPHY

- [1] S. Rodriguez, *1 in 10 in a survey think html is an std - los angeles times*, Mar. 2014. [Online]. Available: <https://www.latimes.com/business/technology/la-fi-tn-1-10-americans-html-std-study-finds-20140304-story.html>.
- [2] M. Eeckhaut and V. Nikolas, *Nsa hackt belgische cyberprof - de standaard*, 2014. [Online]. Available: https://www.standaard.be/cnt/dmf20140131_049.
- [3] S. Derix, G. Greenwald, and H. Modderkolk, *Aivd hackt internetfora, 'tegen wet in' - nrc*, 2013. [Online]. Available: <https://www.nrc.nl/nieuws/2013/11/30/aivd-hackt-internetfora-tegen-wet-in-a1429283>.
- [4] F. Johannès and J. Follorou, *Révélations sur le big brother français*, Jul. 2013. [Online]. Available: https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.
- [5] D. Ford, *Docs shielded cheney defibrillator from hacks - cnn*, Oct. 2013. [Online]. Available: <https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html>.